

Doble Autenticación de Acceso Identificado

Descripción del Sistema de Doble Autenticación

¿Qué es el Segundo Factor de Autenticación?

Es un nuevo protocolo de seguridad implantado por la Universidad de Granada para la protección de datos de carácter personal, que sirve para verificar la identidad del usuario. De esta manera, a partir de ahora, a los usuarios que se autentifiquen en el Acceso Identificado, el sistema les solicitará introducir un código adicional que recibirán de forma inmediata en correo electrónico o teléfono móvil. A este código se le conoce como Doble Factor de Autenticación.

¿Por qué se solicita este Segundo Factor de Autenticación?

La Universidad de Granada está certificada en cumplimiento con el Esquema Nacional de Seguridad, a partir de ahora ENS, Real Decreto 3/2010. Dentro del ENS aparecen unas medidas de protección que hemos de cumplir. Con el tipo de certificación obtenida, "categoría media", se nos pide que pongamos en la autenticación un doble factor para asegurar la identidad de la persona que hace uso del servicio.

Todas las administraciones públicas deben cumplir el ENS, actualmente todas se están adecuando al sistema cl@ve, nosotros de momento utilizamos un método que nos ha parecido menos restrictivo.

Según estudios se ha demostrado que la protección solo con password ya no es segura, es cuestión de tiempo romperla. Con el segundo factor de autenticación aumentamos la seguridad.

¿Me van a solicitar el código de Segundo Factor de Autenticación siempre que acceda mediante Acceso Identificado?

Después de identificarse por primera vez mediante el Segundo Factor, puede evitar que el sistema le requiera el código de verificación durante un mes marcando la casilla correspondiente que le aparecerá en pantalla. Con ello, el sistema estará reconociendo su dispositivo como un equipo de confianza.

Transcurrido un mes, por seguridad, el sistema le volverá a requerir el código de Segundo Factor.

¿Cómo se configura el Segundo Factor de Autenticación?

Si dispone de cuenta de correo de la UGR, la recepción del código de verificación se realizará por defecto en esta cuenta. Pero también deberá elegir una segunda vía para la verificación, optando por la forma que le resulte más cómoda, entre las siguientes posibilidades:

- Otra cuenta de correo personal diferente a la de la UGR.
- Identificación mediante el número del código de barras de su tarjeta universitaria TUI UGR.
- Recepción del código de verificación en su teléfono móvil mediante SMS.

No obstante, puede cambiar su configuración de medios de recepción de la clave del Segundo Factor de Autenticación en cualquier momento utilizando el botón "Configuración" que encontrará en la parte superior de la pantalla de Acceso Identificado.

¿Cómo accedo si aún no tengo cuenta de correo personal de la UGR?

En el caso de que aún no disponga de una cuenta de correo de la UGR, deberá elegir como medio para la recepción de la clave del segundo factor de autenticación otra cuenta de correo personal o su teléfono móvil. En el caso de que cree automáticamente una nueva cuenta de correo de la UGR, ésta se configurará como un medio más para la recepción de dicho código.

¿Puedo cambiar la configuración de medios elegidos por defecto para la recepción del código?

Si, puede cambiar su configuración de medios de recepción de la clave del Segundo Factor de Autenticación en cualquier momento utilizando el botón "Configuración" que encontrará en la parte superior de la pantalla de Acceso Identificado.

Funcionamiento del Sistema de Doble Autenticación

1.- Configuración Inicial

Cuando al usuario se le activa la doble autenticación (la activación la vamos a ir haciendo de forma progresiva para no meter a todos de golpe) la primera vez que entra en Acceso Identificado, tras autenticarse con su usuario y password, el sistema le envía a las pantallas de configuración de la doble autenticación:

Primera Pantalla

Es una pantalla informativa, en la que se explica al usuario como funciona la doble autenticación y el motivo para implantarla. El usuario no tiene que hacer nada, solo pulsar el botón "Siguiente":

Configuración de Segundo factor de Autenticación

¿Qué es el Segundo Factor de Autenticación

Es un nuevo protocolo de seguridad implantado por la Universidad de Granada para la protección de datos de carácter personal, que sirve para verificar la identidad del usuario. De esta manera, a partir de ahora, a los usuarios que se autentifiquen en el Acceso Identificado, el sistema les solicitará introducir un código adicional que recibirán de forma inmediata en correo electrónico o teléfono móvil. A este código se le conoce como Doble Factor de Autenticación.

¿Por qué se solicita este Segundo Factor de Autenticación?

La Universidad de Granada está certificada en cumplimiento con el Esquema Nacional de Seguridad, a partir de ahora ENS, Real Decreto 3/2010. Dentro del ENS aparecen unas medidas de protección que hemos de cumplir. Con el tipo de certificación obtenida, *categoría media*, se nos pide que pongamos en la autenticación un doble factor para asegurar la identidad de la persona que hace uso del servicio.

Todas las administraciones públicas deben cumplir el ENS, actualmente todas se están adecuando al sistema cl@ve, nosotros de momento utilizamos un método que nos ha parecido menos restrictivo.

Según estudios se ha demostrado que la protección solo con password ya no es segura, es cuestión de tiempo romperla. Con el segundo factor de autenticación aumentamos la seguridad.

¿Me van a solicitar el código de Segundo Factor de Autenticación siempre que acceda mediante Acceso Identificado?

Después de identificarse por primera vez mediante el Segundo Factor, puede evitar que el sistema le requiera el código de verificación durante un mes marcando la casilla correspondiente que le aparecerá en pantalla. Con ello, el sistema estará reconociendo su dispositivo como un equipo de confianza. Transcurrido un mes, por seguridad, el sistema le volverá a requerir el código de Segundo Factor.

¿Cómo se configura el Segundo Factor de Autenticación?

Si dispone de cuenta de correo de la UGR, la recepción del código de verificación se realizará por defecto en esta cuenta. Pero también deberá elegir una segunda vía para la verificación, optando por la forma que le resulte más cómoda, entre las siguientes posibilidades:

- Otra cuenta de correo personal diferente a la de la UGR.
- Identificación mediante el código de barras de su tarjeta universitaria TUI UGR.
- Recepción del código de verificación en su teléfono móvil mediante SMS.

No obstante, puede cambiar su configuración de medios de recepción de la clave del Segundo Factor de Autenticación en cualquier momento utilizando el botón "Configuración" que encontrará en la parte superior de la pantalla de Acceso Identificado.

¿Cómo accedo si aún no tengo cuenta de correo personal de la UGR?

En el caso de que aún no disponga de una cuenta de correo de la UGR, deberá elegir como medio para la recepción de la clave del segundo factor de autenticación otra cuenta de correo personal o su teléfono móvil. En el caso de que cree automáticamente una nueva cuenta de correo de la UGR, esta se configurará como un medio más para la recepción de dicho código.

¿Puedo cambiar la configuración de medios elegidos por defecto para la recepción del código?

Si, puede cambiar su configuración de medios de recepción de la clave del Segundo Factor de Autenticación en cualquier momento utilizando el botón "Configuración" que encontrará en la parte superior de la pantalla de Acceso Identificado.

SIGUIENTE →

Segunda Pantalla

En esta pantalla se le informa de que su cuenta institucional (@ugr.es si es personal o @correo.ugr.es si es alumno), si la tiene, se ha configurado automáticamente para recibir el código del doble factor. También se le solicita que escoja un medio alternativo para recibirlo:



UNIVERSIDAD DE GRANADA

Acceso Identificado

Configuración de Segundo Factor de Autenticación

Configuración Actual

Por defecto la clave que solicitará Acceso Identificado la recibirá en:

- Cuenta de correo institucional (XXX @ugr.es)

Importante

Es necesario que configure un segundo método de envío de la clave para prevenir posibles problemas al acceder a su correo electrónico para consultar la clave que le será enviada.

Indique un medio de envío alternativo a su correo institucional:

- Correo Electrónico Externo (distinto a su correo personal @ugr.es)
- Teléfono Móvil mediante el envío de un SMS
- Código numérico de Tarjeta Universitaria TUI UGR

SIGUIENTE →



Tercera Pantalla

En esta pantalla se le solicita al usuario el teléfono o email no institucional en el que quiere recibir el código. Si ha seleccionado la Tarjeta TUI la pantalla informa de que ese ha sido el medio elegido pero no solicita ningún valor:

 UNIVERSIDAD DE GRANADA

Acceso Identificado

Configuración de Segundo factor de Autenticación

A continuación va a configurar donde quiere recibir el código para el Segundo Factor de Autenticación.

Importante:
El valor introducido únicamente se utilizará para recibir el código de doble autenticación de Acceso Identificado.

Número del teléfono móvil en el que desea recibir el SMS:

(Teléfono de 9 dígitos)

SIGUIENTE →



Cuarta Pantalla

Se solicita al usuario el valor de un código que se ha enviado al medio elegido para comprobar que es válido. Si el usuario ha elegido Tarjeta TUI se le pedirán las cifras de 4 posiciones aleatorias del número que aparece bajo el código de barras de la misma:

UNIVERSIDAD DE GRANADA

Acceso Identificado

Configuración de Segundo factor de Autenticación

Para comprobar que ha introducido correctamente el medio de recepción de la clave para el segundo factor de autenticación se ha enviado una clave al **Teléfono (SMS)** que está configurando.

Valor recibido en XXXXX :

Importante: Tenga en cuenta que el SMS puede demorarse unos segundos en llegar

SIGUIENTE →

¿Ha pasado más de un minuto y no ha recibido el código en XXXXXX ?

[Reenviar Clave](#) Quedan 2 intentos

CSIRC | CENTRO DE SERVICIOS DE INFORMÁTICA Y REDES DE COMUNICACIONES

[Conformidad ENS](#) | [Política de Privacidad](#)

En esta pantalla el usuario tiene la opción de reenviar la clave (hasta 3 intentos contando el inicial) por si el mensaje con la clave no ha llegado.

Quinta Pantalla

En esta pantalla se comprueba que la clave introducida es correcta, con lo que damos por válido el valor de teléfono o email introducido. La pantalla pregunta al usuario por el método que quiere usar por defecto (si tiene cuenta institucional, si no tuviera solo tendrían el método que acaban de configurar) y solicita la clave de Acceso Identificado para validar al usuario antes de grabar la configuración:

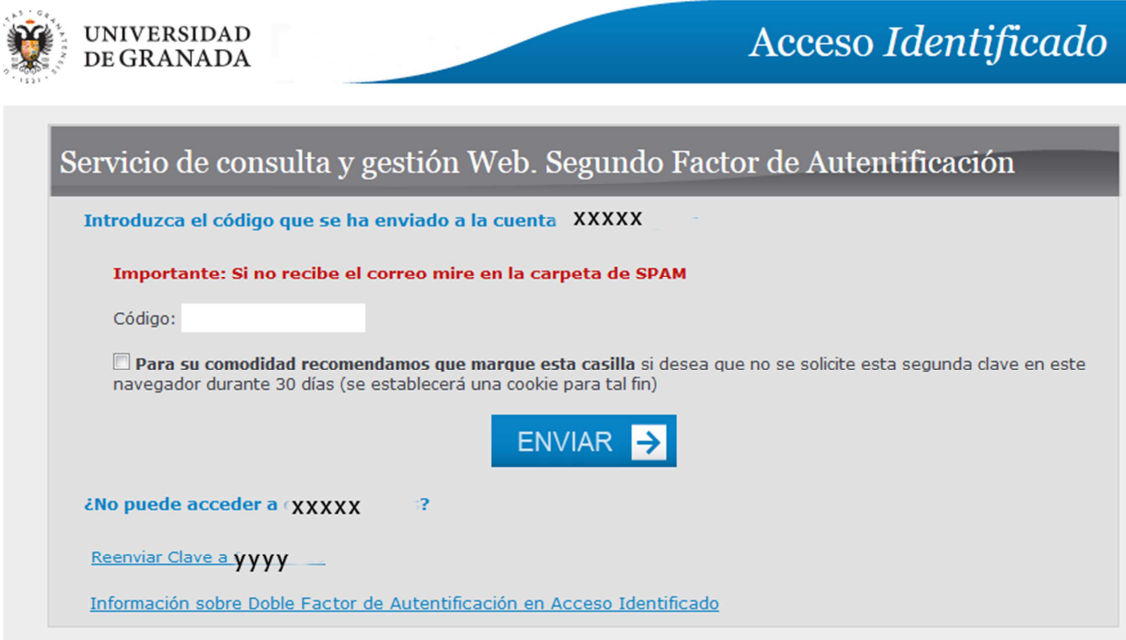
The screenshot shows the 'Configuración de Segundo factor de Autenticación' (Second Factor Authentication Configuration) screen. At the top left is the Universidad de Granada logo. The page title is 'Acceso Identificado'. The main heading is 'Configuración de Segundo factor de Autenticación'. Below this, a message states: 'La validación ha sido correcta. Se va a proceder a grabar su nuevo medio de envío del segundo factor de Autenticación para el Acceso Identificado de la Universidad de Granada. Los datos que se van a grabar son:'. A list of data to be saved includes: 'Medio de Envío: Teléfono Móvil mediante el envío de un SMS' and 'Valor: XXXXXXXX'. Under the heading 'Medio de Envío Predeterminado:', the user is asked to select the default method. Three options are shown: 'Cuenta de Correo Institucional (XXXXXXXX)' with a selected radio button, 'Teléfono (SMS)(XXXXXXXX)' with an unselected radio button, and 'Clave de Acceso Identificado:' followed by a text input field. A blue button labeled 'SIGUIENTE' with a right-pointing arrow is at the bottom center.



Si la validación de la clave fuera incorrecta aparecería un mensaje indicándoselo al usuario y un botón para empezar otra vez el proceso de configuración.

2.- Solicitud de la clave de doble factor cuando el usuario entra a Acceso Identificado

Cada vez que el usuario entra en Acceso Identificado y, tras introducir su usuario y clave y que el sistema valide que son correctos, se mostrará la siguiente pantalla:



The screenshot shows the 'Segundo Factor de Autenticación' (Second Factor Authentication) page. At the top left is the University of Granada logo and name. At the top right is the 'Acceso Identificado' header. The main content area has a title 'Servicio de consulta y gestión Web. Segundo Factor de Autenticación'. Below the title, it says 'Introduzca el código que se ha enviado a la cuenta XXXXX'. A red warning message states: 'Importante: Si no recibe el correo mire en la carpeta de SPAM'. There is a text input field labeled 'Código:'. Below the field is a checkbox with the text: 'Para su comodidad recomendamos que marque esta casilla si desea que no se solicite esta segunda clave en este navegador durante 30 días (se establecerá una cookie para tal fin)'. A blue 'ENVIAR' button with a right arrow is positioned below the checkbox. At the bottom left, there is a link: '¿No puede acceder a XXXXX?'. Below that is another link: 'Reenviar Clave a yyyy'. At the bottom, there is a link: 'Información sobre Doble Factor de Autenticación en Acceso Identificado'.

En el campo código el usuario introducirá el código que ha recibido en xxxxx, que puede ser una dirección de correo, un teléfono o 4 posiciones aleatorias del número que hay bajo el código de barras de la tarjeta TUI, según haya elegido el propio usuario en su configuración.

El campo Checkbox que encontramos debajo permite establecer una cookie en el navegador para que no se pida la clave del segundo factor durante un mes en su navegador. Debemos aconsejar al usuario que por su comodidad lo marquen. IMPORTANTE: esto solo funciona si el usuario tiene habilitadas las cookies y no tiene puesto que se borren cada vez que cierra el navegador.

Si el usuario no pudiera acceder al medio xxxxx (por ejemplo, el medio por defecto es su cuenta de correo institucional y ha olvidado la clave) esta página muestra el enlace "Reenviar clave a yyyy" que permite reenviar la clave al segundo medio que tendrá configurado.

IMPORTANTE: los usuarios que aún no han creado su cuenta institucional solo tienen un medio configurado, por lo que no tendrán esta posibilidad. Cuando estos usuarios se creen su cuenta institucional automáticamente se configurará como el medio por defecto para recibir la clave de doble autenticación.

3.- Modificar la configuración para recibir la clave de doble autenticación

En la parte superior de Acceso Identificado aparecer un nuevo botón, “Configurar”, que permite modificar la configuración de la doble autenticación:



The screenshot shows the top navigation bar of the 'Acceso Identificado' system. The header includes the Universidad de Granada logo and name, and the text 'Acceso Identificado'. Below the header is a navigation menu with buttons for 'Inicio', 'Cambiar Clave', 'Configuración', 'Contacto', 'Ayuda', and 'Salir'. The main content area is titled 'Aplicaciones' and contains a table of application links.

Aplicación	Área	Favorito
Administración de Acceso Identificado	Trámites CSIRC	★
Consulta de Nómina	Servicios	★
Cursos y Alta Deportiva	Servicios	★
Gestión de cuentas de correo CSIRC	Trámites CSIRC	★
Incidencias y Peticiones (C.S.I.R.C.)	Trámites CSIRC	★

Al pulsar el botón aparece una pantalla con los medios configurados, la posibilidad de modificar el medio “configurable” (el que no es la cuenta institucional) y la posibilidad de cambiar el medio predeterminado para recibir la clave:



The screenshot shows the 'Configuración de Segundo factor de Autenticación' screen. It displays the current configuration for the second authentication factor. The configuration is shown in a table with columns for 'Medio', 'Valor', 'Predeterminado', and 'Acciones'. Below the table, there is a question '¿Desea cambiar su medio de envío predeterminado?' and a button 'Cambiar Predeterminado'.

Medio	Valor	Predeterminado	Acciones
Teléfono Móvil mediante el envío de un SMS	999999999	No	Modificar
Correo Electrónico institucional	xxx@ugr.es	Sí	

¿Desea cambiar su medio de envío predeterminado?

Cambiar Predeterminado